Ann Marie Mortimer (SBN 169077)
amortimer@hunton.com
Jason J. Kim (SBN 221476)
kimj@hunton.com
Kirk A. Hornbeck (SBN 241708)
khornbeck@hunton.com
HUNTON & WILLIAMS LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627
Telephone: (213) 532-2000
Facsimile: (213) 532-2020

Samuel A. Danon (admitted *pro hac vice*)
sdanon@hunton.com
John J. Delionado (admitted *pro hac vice*)
jdelionado@hunton.com
HUNTON & WILLIAMS LLP
1111 Brickell Avenue, Suite 2500
Miami, Florida 33143
Telephone: (305) 810-2500
Facsimile: (305) 810-2460

Attorneys for Defendants
Yahoo! Inc. and
Aabaco Small Business, LLC

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA - SAN JOSE DIVISION

IN RE: YAHOO! CUSTOMER DATA SECURITY BREACH LITIGATION

CASE NO.: 16-MD-02752-LHK

DEFENDANTS YAHOO! INC. AND AABACO SMALL BUSINESS, LLC'S:

(1) NOTICE OF MOTION AND MOTION TO DISMISS; AND

(2) MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT THEREOF

[Request for Judicial Notice and [Proposed] Order filed concurrently herewith]

Date: August 24, 2017
Time: 1:30 p.m.
Courtroom: 8, 4th Floor
Judge: Hon. Lucy H. Koh

TO ALL PARTIES AND THEIR COUNSEL OF RECORD:

PLEASE TAKE NOTICE THAT, on August 24, 2017, at 1:30 p.m., or as soon thereafter as this matter may be heard before the Honorable Lucy H. Koh, in Courtroom 8 of the United States District Court of California, located at 280 South First Street, 4th Floor, San Jose, California 95113, Defendants Yahoo! Inc. ("Yahoo") and Aabaco Small Business, LLC ("Aabaco") (together, "Defendants") will and hereby do move this Court for an order dismissing Plaintiffs' Consolidated Class Action Complaint (the "Complaint") in its entirety.

This Motion is made on multiple grounds under Rules 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure:

First, each of Plaintiffs' claims fails because they have not and cannot plausibly allege any injury or damages, much less injury or damages that are traceable to Defendants' alleged conduct—requisite elements of Article III standing and each of the claims.

Second, Plaintiffs fail to state a claim under California's unfair competition laws, as they have not pled any unlawful, unfair, or fraudulent conduct on the part of Defendants. Nor can they obtain the remedies sought.

Third, Plaintiffs fail to state a claim under the Consumer Legal Remedies Act ("CLRA"). Plaintiffs are not "consumers" under the statute, as they did not "purchase or lease" a covered "good" or "service" under the CLRA. Plaintiffs also have failed to plead fraudulent conduct on the part of Yahoo, much less with the requisite degree of particularity.

Fourth, Plaintiffs fail to state a claim under the Customer Records Act ("CRA"). As an initial matter, the non-California resident Plaintiffs lack statutory standing under the CRA. Similarly, CRA notice was not required in connection with the alleged 2013 Breach, as the CRA did not cover "online account" information at that time. Likewise, the CRA does not apply to the Forged Cookie Breach, as it did not expose any covered information. Moreover, Plaintiffs fail to allege notification-delay damages—rather, Plaintiffs merely purport to allege damages resulting from the alleged breaches themselves. Plaintiffs' requested statutory penalties under Section 1798.84(c) of the Civil Code are unavailable, as those penalties are limited to alleged violations of

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

California's "Shine the Light" law (which Plaintiffs do not plead). Last, Plaintiffs plead no basis for injunctive relief in connection with alleged harms flowing from past breaches.

Fifth, Plaintiffs fail to state a claim under the Stored Communications Act ("SCA"), as Defendants did not "knowingly" divulge Plaintiffs' alleged information; Plaintiffs admit it was stolen by third parties. Similarly, the alleged Forged Cookie Breach falls outside the ambit of the SCA, as none of the information contained in the cookies included covered "content."

Sixth, Plaintiffs fail to state a claim under Online Privacy Protection Act ("OPPA"), which does not provide a private right of action. Beyond that, OPPA applies only to California residents, which excludes Essar, the Ridolfos, Garg, Rivlin, Granot and Neff. And the only two remaining Plaintiffs fail to state a claim nonetheless because they are not "consumers"—they did not "purchase or lease" anything from Yahoo.

Seventh, Plaintiffs fail to state a claim under any of their contract theories. They have not alleged a breach of any express or implied terms; nor can they use an implied covenant theory to impose new obligations on Defendants. Even still, Plaintiffs cannot plead the requisite damages, as any consequential damages flowing from the alleged breaches are barred under the terms of service to which Plaintiffs agreed.

Eighth, Plaintiff Brian Neff fails to state a claim for fraudulent inducement, as he fails to plead any actionable fraud or reliance, much less with the requisite particularity.

Ninth, Plaintiffs' negligence theories—negligent misrepresentation and negligence—fail under the economic loss rule.

Tenth, Plaintiffs cannot bring claims on behalf of the Australia, Venezuela and Spain Classes, as those individuals are bound by terms of service that require them to bring their claims under different laws and in different fora.

Finally, Plaintiffs have not pled entitlement to declaratory relief. Their conclusory assertions that provisions in Defendants' respective terms of service are "unconscionable and unenforceable" are just that.

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

This Motion will be based upon this Notice of Motion and Motion, the accompanying Memorandum of Points and Authorities, the Request for Judicial Notice filed concurrently herewith, the pleadings and papers on file, and upon such oral argument as may be made at the hearing.

Dated: May 22, 2017

HUNTON & WILLIAMS LLP

By: /s/ Ann Marie Mortimer
Ann Marie Mortimer
Attorneys for Defendants
Yahoo! Inc. and Aabaco Small Business, LLC

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

TABLE OF CONTENTS

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

TABLE OF AUTHORITIES

Page(s)

Cases

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Statutes

Rules

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

This litigation arises out of one of the most organized, sophisticated and relentless criminal attacks in cybercrime history, sponsored by the Russian Federal Security Service (the successor of the infamous "KGB"), and executed by a veritable "who's who" of cybercriminals, including members of the FBI's "Most Wanted" list and Interpol's Red Notice. This was no ordinary security breach, but a full-fledged, state-sponsored cyber assault designed to evade Yahoo! Inc.'s ("Yahoo") security measures, avoid Yahoo's detection systems, and adapt and evolve to meet Yahoo's security defenses and upgrades. With Yahoo's cooperation and assistance, the Department of Justice ("DOJ") was able to identify and indict the perpetrators, the first time foreign government officials have ever been charged in the United States for cybercrime. After the indictment, the United States Attorney for this very District stated: "We commend Yahoo … for providing exemplary cooperation while zealously protecting [its] users' privacy."[1]

The crime perpetrated against Yahoo and its users was not a simple failure in security, as Plaintiffs have suggested, but rather a triumph of criminal persistence, ultimately thwarted only by dogged law enforcement investigation and Yahoo's cooperation. Plaintiffs nevertheless attempt to turn this criminal intrusion on its head and make Yahoo responsible for these sophisticated criminal acts because it allegedly "represented and warranted to Plaintiffs and Class Members that its PII databases were secure and that customers' PII would remain private." Compl. ¶ 34. But Plaintiffs can make this assertion only by wrenching Yahoo's clear statements wholly out of context. Indeed, as is widely understood by Internet users, no security system is hack-proof, and Yahoo specifically warned its users that the Internet is not "100% secure" and that all security measures are limited. In a world in which information stored, transmitted and shared across the Internet is constantly vulnerable to criminal intrusion and security breaches by multiple sources, the burden is on Plaintiffs, at the very least, to plausibly demonstrate concrete injuries that were actually caused by

[1] Request for Judicial Notice ("RJN"), Exh. J, at 2, https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.

Yahoo and not some other source. Plaintiffs do not do this, and their claims fail for multiple distinct reasons.

First, Plaintiffs have not satisfied their threshold burden of demonstrating Article III standing. To start, Plaintiffs have failed to plead actual, plausible and concrete injuries caused by Yahoo. Reimbursed expenses, loss of personal identifying information ("PII") value and other highly individualized "harms" are not sufficient to support standing. Moreover, the alleged harms Plaintiffs claim stem from information disseminated by Plaintiffs to third parties, *not* information collected and stored by Yahoo on its network, and Plaintiffs fail to draw *any* causal connection between the highly individualized injuries alleged (from the filing of fraudulent tax returns to various financial frauds) and the Yahoo breaches, as opposed to the numerous other potential causes of the events. Among other things, Plaintiffs fail to allege their passwords or security questions were decrypted or unhashed, their security questions were correlated to their email addresses, or their accounts were subject to specific cookie forgery that would allow access to those accounts. Instead, Plaintiffs' allegations are riddled with factual blanks and filled with causal holes. This dooms all of Plaintiffs' claims under Rule 12(b)(1).

Second, the Complaint should be dismissed in its entirety under Rule 12(b)(6). As an initial matter, Plaintiffs fail to meet the heightened pleading standard that governs their Unfair Competition Law ("UCL"), Consumers Legal Remedies Act ("CLRA") and fraud-based claims. Similarly, Plaintiffs fail to plead any unlawful, unfair, or fraudulent conduct on the part of Defendants, as required by the UCL, and they cannot obtain the remedies sought thereunder. Likewise, Plaintiffs are not "consumers" who "purchased" or "leased" a covered "good" or "service" under the CLRA. Additionally, Plaintiffs' Customer Records Act ("CRA") claim is limited to California residents, and fails even as to that limited sliver of a putative class because, among other things, no notice was required for the 2013 breach, no damages were specifically attributable to any alleged breach-notification delay, and Plaintiffs have no claim for statutory damages related to the "Shine the Light" provision of the CRA, which Plaintiffs do not even allege applies here. Plaintiffs' other statutory claims are likewise flawed. Plaintiffs have failed to plead a willful and intentional disclosure sufficient to state a claim under the Stored Communications Act ("SCA"), and the Online Privacy

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Protection Act ("OPPA") has no private right of action. Plaintiffs cannot allege a breach of any specific express or implied contractual promise, and cannot use the implied covenant to rewrite Yahoo's Terms of Service and create a promise of absolute security. Plaintiffs' claim for negligence is brought on behalf of foreign nationals who should not be part of this lawsuit, and it is barred by the economic loss doctrine in any event. Lastly, Plaintiffs' declaratory relief claim consists of bare legal conclusions and attempts to create a claim out of an anticipated legal defense. For all of these reasons and more, Plaintiffs' Complaint fails.

II. STATEMENT OF ISSUES TO BE DECIDED

1. Whether Plaintiffs' Complaint demonstrates the requisite injury-in-fact and causation sufficient to confer Article III standing;

2. Whether Plaintiffs' Complaint otherwise states plausible claims for relief;

3. Whether the foreign Plaintiffs are barred from pursuing their negligence claim under California law and in this forum.

III. FACTUAL BACKGROUND

Yahoo provides free[2] web-based email services to its consumer users, subject to certain Terms of Service ("TOS") which define the relationship between Yahoo and its users, and which expressly disclaim the very legal theories Plaintiffs advance here. The TOS repeatedly and expressly disavows any representation that transmission over the Internet is, or could be, totally secure. Instead, Defendants' TOS and incorporated Privacy Policies explained that any use of the services would be "AT YOUR OWN RISK" and on an "AS IS" and "AS AVAILABLE" basis, they expressly disclaim any warranties to the contrary, including that transmission using the services would be "SECURE,"[3] and they explicitly warn that "[n]o data transmission over the Internet or

[2] Only Plaintiffs Neff and Rivlin claim to have paid fees to Defendants. Neff paid fees solely in connection with his alleged use of Defendants' small business services. The TOS to which Neff agreed is near-identical in all material respects to the TOS that governs Yahoo's relationship with its free users, including the same or similar warranty disclaimers and admonitions regarding security limitations. And Rivlin allegedly paid for an email forwarding service only, which was not alleged to have been impacted by the data breaches in any way.

[3] Compl., Exh. 1, at 91 § 19(a) & (b); Compl., Exh. 2, at 171 § 12(a) & (d).

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

information storage technology can be guaranteed to be 100% secure,"[4] and that all security measures, including the "SECURITY MECHANISMS IN THE SERVICES HAVE INHERENT LIMITATIONS."[5]

- ***The "2014 Breach":*** In late 2014, a copy of certain user account information was stolen from Yahoo's networks in a state-sponsored attack by Russia, originally targeting the emails of "Russian journalists, U.S. and Russian government officials and private-sector employees of financial, transportation and other companies."[6] Yahoo took remedial actions in response; among other things, it notified 26 specifically targeted users and consulted with law enforcement.[7] In late July 2016, a hacker claimed to have obtained certain Yahoo user data, and, on August 1, 2016, the media reported a hacker's claim that he had obtained certain user account details associated with 200 million Yahoo users from "2012 most likely." J. Cox, "*Yahoo 'Aware' Hacker Is Advertising 200 Million Supposed Accounts on Dark Web*," Vice Motherboard, (Aug. 1, 2016), available at http://motherboard.vice.com/read/yahoo-supposed-data-breach-200-million-credentials-dark-web. After investigating the claim with the assistance of outside forensic experts, Yahoo was unable to substantiate the claim. However, Yahoo's internal security personnel intensified an ongoing broad review of Yahoo's network and data security, including a review of historical information related to the potential exfiltration of user records. Based upon this investigation, Yahoo disclosed that the 2014 intrusion impacted additional users and information, including in some instances names, email addresses, telephone numbers, dates of birth, hashed passwords (most encrypted with bcrypt[8]), and some encrypted or unencrypted security questions and answers. There was no evidence that any unprotected passwords or payment-card data was accessed from any network system, and this type of financial data is not routinely collected or stored by Yahoo in connection with its free email

[4] RJN, Exh. A, at 1, https://policies.yahoo.com/us/en/yahoo/privacy/topics/security/.

[5] Compl., Exh. 2, at 171 § 12(c).

[6] *Supra* note 1.

[7] RJN, Exh. G, at 48, Yahoo! Inc., Annual Report (Form 10-K), 47 (Mar. 1, 2017).

[8] Yahoo notified users that the stolen information did not include unprotected passwords, and that the vast majority were encrypted with bcrypt, now considered an industry standard. RJN, Exh. E, at 1, https://investor.yahoo.net/releasedetail.cfm?ReleaseID=990570.

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

services.[9] On September 22, 2016, Yahoo provided notice to potentially affected users and took additional steps to secure user accounts—*e.g.*, recommending that users change their passwords and invalidating unencrypted security questions and answers.[10] Within days of Yahoo's announcement, the first of 31 lawsuits were filed in federal court, all of which were consolidated into this MDL. Plaintiffs refer to this as the "2014 Breach."

In conjunction with Yahoo's internal security review, and understanding the sophistication of the intrusion itself, Yahoo's Board of Directors also commissioned an internal investigation by an Independent Committee to better understand the scope of the intrusion, and Yahoo's detection and response to it. In its March 1, 2017 10-K, with the benefit of a full forensic investigation and a thorough independent investigation of the intruder activity in 2014 and following, the Company disclosed the Committee's conclusion that, as of December 2014, Yahoo's "information security team understood that [an] attacker had exfiltrated copies of user database backup files" in connection with the 2014 Breach.[11] The focus of the information security team during 2014 was on expelling the Russian intruders from Yahoo's network systems, and it is "unclear whether and to what extent such evidence of exfiltration was effectively communicated and understood outside the information security team," and the Committee "did not conclude that there was an intentional suppression of relevant information."[12] And although certain aspects of the intrusion were detected by the information security team earlier, as the DOJ noted, it took a "highly complicated investigation of a very complex threat" to uncover and appreciate the full scope of the intrusion.[13]

- ***The "Forged Cookie Breach":*** As part of the investigation into the 2014 Breach, Yahoo discovered that the same Russian state-sponsored actors behind the 2014 Breach also created cookies for a specific subset of the Yahoo user population, which may have been used to access certain users' accounts or account information in 2015 and 2016. Plaintiffs refer to this as the "Forged

[9] RJN, Exh. H, at 44, Yahoo! Inc., Quarterly Report (Form 10-Q), 43 (May 9, 2017).

[10] *Supra* note 8.

[11] *Supra* note 7.

[12] *Id.*

[13] *Supra* note 1.

Cookie Breach," but do not specifically allege any named Plaintiff was impacted by, or received notice of, the Forged Cookie Breach.

- ***The "2013 Breach":*** After the September announcement, Yahoo received evidence from law enforcement of a separate and earlier breach by unrelated criminal intruders. Additional investigation with outside forensic experts determined that this breach likely occurred in or around August 2013. As with the previously announced breach, this intrusion did not implicate "unhashed" passwords in clear text,[14] payment card data, or bank account information that Plaintiffs otherwise did not disclose themselves to third parties.[15] Nonetheless, Yahoo notified users of the need to change their passwords.[16] Plaintiffs refer to this breach as the "2013 Breach" and specifically allege that it was "too late" to improve security after this breach.[17] Compl. ¶ 56.

Although Plaintiffs suggest Yahoo could have, and should have, detected and understood the full scope of these criminal intrusions earlier, they ignore both the stealth and sophistication of the perpetrators. As the DOJ emphasized, the criminal activity "targeted" Yahoo, was "beyond the pale," and, because of the involvement of Russia, was not a "fair fight" and, as importantly, not a fight Yahoo could "win alone."[18] Moreover, in the face of a "very complex threat," the DOJ publicly "commend[ed] Yahoo … for their sustained and invaluable cooperation in the investigation aimed at obtaining justice for, and protecting the privacy of their users."[19] Indeed, former Acting Assistant Attorney General Mary B. McCord personally "thank[ed] Yahoo …, whose customers were targeted, and who cooperated with us."[20]

[14] At the time, many of those passwords would have been "hashed" using the MD5 algorithm. The "hashing" process converted the passwords into unreadable strings of characters.

[15] RJN, Exh. F, at 1, https://investor.yahoo.net/releasedetail.cfm?ReleaseID=1004285.

[16] *Id.*

[17] The 2013, 2014 and Forged Cookie Breaches are referred to collectively as the "Data Breaches."

[18] *Supra* note 1, at 1; RJN, Exh. K, at 2, https://www.justice.gov/opa/speech/acting-assistant-attorney-general-mary-b-mccord-delivers-remarks-press-conference.

[19] *Supra* note 1, at 1-2.

[20] RJN, Exh. K, at 2, https://www.justice.gov/opa/speech/acting-assistant-attorney-general-mary-b-mccord-delivers-remarks-press-conference.

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

IV. LEGAL ARGUMENT

Plaintiffs' claims fail at the outset for lack of standing. Plaintiffs fail to allege the sort of concrete and particularized harms necessary to show injury-in-fact. And even if Plaintiffs could establish injury-in-fact (and they cannot), Plaintiffs fail to trace those alleged "injuries" to Defendants' conduct. There are no facts showing how the alleged disclosure of—in many cases, non-specified—information resulted in Plaintiffs' alleged injuries. Plaintiffs' pleading problems, however, do not end with their inability to establish standing. Each of their claims also fails to set forth plausible bases for relief under Rule 12(b)(6), and certain foreign Plaintiffs' claims also must be dismissed under the *forum non conveniens* doctrine.

A. Plaintiffs Fail To Meet Their Threshold Burden Under Article III.

When a party moves under Rule 12(b)(1) for lack of subject-matter jurisdiction, "the opposing party bears the burden of establishing the court's jurisdiction." *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1208 (N.D. Cal. 2014) (quotations omitted). "A suit brought by a plaintiff without Article III standing is not a 'case or controversy,' and an Article III federal court therefore lacks subject-matter jurisdiction over the suit." *Cetacean Cmty. v. Bush*, 386 F.3d 1169, 1174 (9th Cir. 2004). A plaintiff bears the burden of establishing: (1) a concrete injury-in-fact (2) that is fairly traceable to defendant's challenged conduct and (3) likely to be redressed by a favorable decision. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61 (1992). Embedded in Article III standing is the requirement that the complained-of harm is causally connected to the alleged wrongdoing and fairly traceable to the defendant's conduct, not the "independent action of some third party not before the court." *Id.* at 560 (quotations and citations omitted). "Article III standing is also claim- and relief-specific, such that a plaintiff must establish Article III standing for each of her claims and for each form of relief sought." *Adobe*, 66 F. Supp. 3d. at 1218 (citing *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 352 (2006)). Importantly, "Article III's standing requirements are mandatory and separate from any statutory standing requirements." *Id.* Thus, a "plaintiff may satisfy the injury-in-fact requirements to have standing under Article III," but nonetheless lack the requisite statutory standing to be "able to assert a cause of action successfully." *Low v. LinkedIn Corp.* ("*Low*

II"), 900 F. Supp. 2d 1010, 1020 (N.D. Cal. 2012) (quotations omitted). Plaintiffs fail to establish Article III standing for any claims, much less every claim.

1. Plaintiffs Fail To Allege Injury-In-Fact Sufficient To Show Standing.

To establish standing, a plaintiff must first demonstrate an "injury-in-fact that is concrete and particularized, as well as actual and imminent." *Low v. LinkedIn Corp.* (*"Low I"*), 2011 WL 5509848, at *2 (N.D. Cal. Nov. 11, 2011) (dismissing data disclosure case due to lack of standing). Plaintiffs fail to make this threshold showing and instead take a scattershot approach by alleging highly individualized, but overly hypothetical alleged harms:

- ***Loss of value of PII:*** Plaintiffs generally claim that the Data Breaches caused the loss of value of various types of personal information because unspecified information was allegedly for sale on the "Dark Web" and otherwise has value to criminals. Compl. ¶¶ 145, 157, 184, 188, 195. However, loss of "PII value" due to disclosure has been held to be "too abstract and hypothetical to support Article III standing." *Low I*, 2011 WL 5509848, at *2; *see also Fernandez v. Leidos, Inc.*, 127 F. Supp. 3d 1078, 1089 (E.D. Cal. 2015) ("Plaintiff has not shown he has standing to bring his claims based on his allegation that he has been deprived of the value of his PII/PHI."). Nor have Plaintiffs alleged that they have attempted to monetize, or are foreclosed from monetizing, their own PII as a result of the Data Breaches. *In re Google Android Consumer Privacy Litig.*, 2013 WL 1283236, at *4 (N.D. Cal. Mar. 26, 2013) ("Plaintiffs also do not allege they attempted to sell their personal information, that they would do so in the future, or that they were foreclosed from entering into a value for value transaction relating to their PII, as a result of the Google Defendants' conduct."). And the claimed devaluation of their PII alone does not qualify as a concrete injury sufficient to meet the requirements of standing. *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 954 (D. Nev. 2015) (rejecting plaintiffs' attempt to establish standing by arguing that data breach resulted in devaluation of personal information).
- ***Lost/Unwanted Emails:*** Plaintiffs also complain that they both lost emails and received unwanted emails. Neither qualifies as a concrete, particularized injury for Article III purposes. *Fernandez*, 127 F. Supp. 3d at 1087 (no standing based on lost medical records); *In re Zappos.com, Inc.*, 2016 WL 2637810, at *3 (D. Nev. May 6, 2016) (no standing where data breach plaintiffs

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

alleged "that their email accounts were 'accessed by hackers and used to send unwanted advertisements to people in [their] address book[s]'").

- ***Reimbursed Expenses:*** No Plaintiff alleges unreimbursed fraudulent charges, which is a necessary predicate of concrete harm. In fact, one Plaintiff, Abitol (Compl. ¶ 19), admits he was reimbursed for funds that had been improperly wired from his bank account. This undercuts any claim of actual injury. *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, 2016 WL 6523428, at *4 (S.D. Cal. Nov. 3, 2016) (reimbursed losses do not constitute an "actual injury" for purposes of standing). Plaintiffs' failure to allege actual, unreimbursed fraudulent charges is fatal to their claim of injury and defeats standing. *See Whalen v. Michaels Stores, Inc.*, 2017 WL 1556116, at *2 (2d Cir. May 2, 2017) (affirming dismissal of data breach case for lack of Article III standing when plaintiff alleged no unreimbursed fraudulent charges).

- ***Other "Harms":*** Plaintiffs allege a number of other purported injuries that do not qualify as concrete injuries. For example, the "mere violation of a consumer protection statute [does not] establish a 'concrete' injury." *Dugas*, 2016 WL 6523428, at *6. Plaintiffs also allege additional totally idiosyncratic and highly speculative harms, including fear that a terrorist may impersonate him (Compl. ¶ 11) and fear that Flickr photos will be "exposed" (*id.* ¶ 14), both of which fall well short of the mark to qualify as a concrete, particularized injury. *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1150 (2013) ("We decline to abandon our usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors. … [R]espondents' speculative chain of possibilities does not establish that injury based on potential future [activity] is certainly impending or is fairly traceable."). Similarly, Robles claims hackers "stole business ideas from her e-mail account." Compl. ¶ 17. But that bare allegation lacks sufficient substance and specificity to show injury-in-fact. *See*, *e.g.*, *Whalen*, 2017 WL 1556116, at *2 (affirming dismissal of data breach case for lack of standing, in part, based on vague allegations of injury unsupported by facts).

2. Plaintiffs Fail To Plead Facts Sufficient For Traceability.

Plaintiffs must plausibly plead facts sufficient to connect the causal dots between the information actually exposed in the alleged breach and the harm they claimed to have suffered, such "that the injury is fairly traceable to the challenged action of the defendant." *In re LinkedIn User*

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Privacy Litig., 932 F. Supp. 2d 1089, 1092 (N.D. Cal. 2013) (citing *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000)). In this case, even if the tax return fraud and other "harms" alleged by Plaintiffs qualified as "concrete" and "actual" injuries, Plaintiffs would still have to show the injuries were caused by, and are traceable to, the Data Breaches. Not even the DOJ's 47-count indictment against the hackers alleged the varied misuse of Yahoo user information that Plaintiffs claim here. The mere fact of a criminal intrusion into Yahoo's network and some alleged privacy harm to users of Yahoo's services is not sufficient to demonstrate standing. *Cf. Resnick v. AvMed*, 693 F.3d 1317, 1326 (11th Cir. 2012) ("pleadings must include allegations of a nexus between the [identity theft] beyond allegations of time and sequence"). This is especially true here given the numerous potential causes of the alleged injuries and the temporal distance between the Data Breaches and some of these alleged harms.

a. There Is No Causal Connection Between The Information Stolen And The Injuries Claimed.

Plaintiffs fail to plead the causal nexus necessary to demonstrate traceability. As a starting point, the information allegedly disclosed was not collected or stored by Yahoo on its network. Instead, the only source of this information through Yahoo—if accessed by the intruders at all—was Plaintiffs' own pre-breach communications. But Yahoo and this Court are left to guess how (if at all) the purported harms alleged could be traceable to the Data Breaches, since Plaintiffs fail to plead facts sufficient to link the harm to these breaches rather than, for instance, the pre-breach activities of Plaintiffs, those with whom Plaintiffs communicated, or other breaches unrelated to Yahoo. *See Antman v. Uber Techs., Inc.*, 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015) (allegation that hacker attempted to open credit card in plaintiff's name did not create standing where no allegation that Social Security number was target of breach); *Attias v. CareFirst, Inc.*, 199 F. Supp. 3d 193, 201 (D.D.C. 2016) (alleged tax return fraud was not fairly traceable to data breach when complaint did not allege Social Security numbers were exposed). To the extent Social Security numbers or any other specific personal information were communicated via Yahoo email at all, it was sent out over the Internet to undisclosed recipients, at undisclosed times, with undisclosed frequency, and at risk with each transmission of disclosure from any source and via the medium over which it was sent.

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Nor have Plaintiffs alleged facts suggesting the harms of which they complain can be isolated to the Data Breaches. In all instances, Plaintiffs' references to "PII and financial information" are as intentionally broad as they are vague, and lack the factual underpinnings to causally connect this information—whatever it is—and any resulting harm caused by its use to the Data Breaches. Plaintiffs' failure to allege that the information stolen as a result of the Data Breaches is the same information necessary to cause the injuries alleged undermines their ability to trace the harm alleged to the Data Breaches, and defeats any claim of Article III standing. *Welborn v. Internal Revenue Serv.*, 2016 WL 6495399, at *9 (D.D.C. Nov. 2, 2016) (plaintiffs "must allege facts that indicate that the information stolen … is the same type of information used to commit their injuries").

For example, Dugas and the Ridolfos allege numerous fraudulent charges on various credit cards. Compl. ¶¶ 12, 13. However, Dugas has made the judicial admission that his credit card information was exposed in a different data breach. RJN, Exh. L, at 5-6, *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, 2016 WL 8469592, ¶ 23 (S.D. Cal. Dec. 7, 2016) (Second Am. Class Action Compl. alleging credit card compromise causing Dugas to seek new card issuance and account updates). His conclusory allegation that he suffered financial fraud as a result of the Data Breaches here must therefore be disregarded. Moreover, Dugas fails to allege that any credit card information was stored on the Yahoo network or specifically disclosed by him via Yahoo email, much less that sufficient information necessary to perpetrate credit card fraud was somehow accessible as part of the Data Breaches. Compl. ¶ 12. Similarly, the Ridolfos generally allege that they have information in their Yahoo accounts concerning "general banking, credit card management and communications, [and] mortgage finance," but likewise fail to identify what information they have, where they have it, whether they themselves released that information (and how), how any specific information sufficient to conduct credit card fraud was accessible as part of the Data Breaches, and who else had access to this information. *Id.* ¶ 13. Likewise, although Dugas and Essar both seek to hold Yahoo liable for alleged tax return fraud, neither claims their Social Security numbers—much less any other specific data element needed in combination to commit tax return fraud—were either among the hacked data, or otherwise contained in any of their Yahoo accounts and accessed by hackers. *Id.* ¶¶ 11-12. Given that "[t]ax-related identity theft occurs when

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

someone *uses a stolen Social Security number* to file a tax return claiming a fraudulent refund," the failure to allege exposure of Social Security numbers is fatal. RJN, Exh. I, at 1, IRS Taxpayer Guide to Identity Theft (available at https://www.irs.gov/uac/taxpayer-guide-to-identity-theft) (emphasis added). Additionally, Heines alleges that her Yahoo account contained "information relating to her account with Direct Express, the payment service through which she receives her Social Security benefits," yet she makes no allegation that the account contained information sufficient to divert her monthly disability allowance fraudulently, or how such a diversion could have taken place as a result of the Data Breaches. Compl. ¶ 10; *see also In re Horizon Healthcare Servs., Inc. Data Breach Litig.*, 2015 WL 1472483, at *8 (D.N.J. Mar. 31, 2015) (even if certain information from breached system could be cobbled together with information from other sources to commit fraud, alleged harm was not fairly traceable to breach), *vacated on other grounds*, *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625 (3d Cir. 2017).

Plaintiffs' generalized, non-specific allegations will not do. *Antman* is instructive. In that case, when the plaintiff alleged "disclosure only of his name and drivers' license information," the court found "[i]t is not plausible that a person could apply for a credit card without a Social Security number." *Antman*, 2015 WL 6123054, at *11. Even though the plaintiff also "alludes to the disclosure of unspecified 'other personal information;' this is insufficient" to show traceability. *Id.*; s*ee also Unchageri v. Carefirst of Maryland, Inc.*, 2016 WL 8255012, at *7 (C.D. Ill. Aug. 23, 2016) (denying motion to amend to cure lack of standing when alleged harm not fairly traceable to health insurance database breach: "Plaintiff does not allege or explain how the allegedly unauthorized charges can be traced to the challenged action of Defendants, and not simply the result of an independent action of some third party not before the Court. This is an important point because nowhere in the Complaint or the proposed Amended Complaint does Plaintiff allege credit card or financial information was stolen.").

b. Plaintiffs Have Failed To Plead Facts To Link Breaches From 2013 And 2014 To Injury Today, And Other Causes Exist.

The time elapsed between the Data Breaches and the alleged injuries makes pleading facts plausibly showing traceability and causation more critical. For example, Plaintiffs Essar and Corso claim to have been affected by the 2014 Breach, with purported injuries occurring two or three years

later (in 2016 through 2017, and in 2016, respectively). Compl. ¶¶ 11, 18. Even more tenuous, the Ridolfos and Rivlin claim to be affected by the 2013 Breach, yet allege injuries with a wider gap in time (also occurring in 2016 through 2017, and in 2016, respectively). *Id.* ¶¶ 13, 15. Neff also alleges facts suggesting he was potentially affected by the 2013 Breach, yet claims to have suffered injuries in 2016. *Id.* ¶ 20. Other Plaintiffs (Garg, Granot) fail to allege any dates at all for the alleged injuries. *Id.* ¶¶ 14, 16. Moreover, still other Plaintiffs fail to allege they received any breach notice at all from Yahoo (Dugas, Granot, Robles). *Id.* ¶¶ 12, 16-17. These wide time gaps underscore Plaintiffs' failure to plead facts sufficient to show causal relatedness and attenuate the causal chain beyond the bounds of plausible traceability required by Article III. *See*, *e.g.*, *Duqum v. Scottrade*, *Inc.*, 2016 WL 3683001, at *4 (E.D. Mo. July 12, 2016) (finding lack of temporal connection when more than two years passed since the original data breach).

c. Yahoo Is Not Liable For Theft Of Publicly Available Information.

Nor can Plaintiffs manufacture a traceable injury by complaining about unsolicited mail or advertisements. Compl. ¶¶ 11, 14-16. No Plaintiff has alleged that his or her email address (as well as certain other data elements) was not publicly available and therefore "would have been difficult for marketers [or other persons] to locate absent the assistance of the data thief." *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 33 (D.D.C. 2014) (no traceability for publicly available phone number); *see Fernandez*, 127 F. Supp. 3d at 1086 (no traceability between data breach and increased email and advertisements).

B. <u>Plaintiffs' Claims Fail Under Rule 12(b)(6).</u>

To survive dismissal under Rule 12(b)(6), Plaintiffs must establish a "plausible" basis for relief. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007); *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). And they must do so without the need for the Court to "fill in the blanks" left open by deficient allegations. *Tall v. Ryan*, 1990 WL 68849, at *1 (9th Cir. May 23, 1990). Allegations are not "plausible" if they are "merely consistent with" a defendant's liability or establish no "more than a sheer possibility" of liability. *Iqbal*, 556 U.S. at 678. Moreover, because several of Plaintiffs' claims also sound in fraud, they must meet Rule 9(b)'s heightened pleading standards. *Kearns v.*

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Ford Motor Co., 567 F.3d 1120, 1125 (9th Cir. 2009). Plaintiffs have failed to plead the who, what, when, where, and how of any allegedly fraudulent conduct with particularity. *Id.* at 1124.

1. Plaintiffs Fail To State A Claim For A UCL Violation.

To state a UCL claim, Plaintiffs must plead "with reasonable particularity the facts supporting the statutory elements of the violation." *Khoury v. Maly's of Cal., Inc.*, 14 Cal. App. 4th 612, 619 (1993). Plaintiffs also must demonstrate actual injury caused by the alleged violation. Plaintiffs do not, because they have not pled a loss of money or property, and the injuries alleged are either reimbursed (forged credit and tax returns, fraudulent credit card charges) or otherwise not compensable. Compl. ¶ 135; *see also Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 322 (2011); *supra* Section IV(A); *In re Sci. Applications*, 45 F. Supp. 3d at 26 ("The cost of credit monitoring and other preventative measures, therefore, cannot create standing."). Similarly, because the consumer Plaintiffs paid no money to use Yahoo's free services, there is nothing to refund. *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 714 (N.D. Cal. 2011) (personal information does not constitute property under UCL); *Dugas*, 2016 WL 6523428, at *11 (general averments of unauthorized credit card charges, mitigation/monitoring costs, time spent responding to unauthorized charges, and loss of PII value do not amount to loss of money or property under UCL). Accordingly, Plaintiffs' UCL claims fail for lack of injury alone.

a. Plaintiffs' Allegations Do Not Establish An "Unlawful" Act.

Plaintiffs do not properly plead "unlawful" conduct. Plaintiffs claim Yahoo's practices were unlawful because they allegedly violated the CLRA, CRA, SCA and OPPA. Compl. ¶¶ 134, 221. As shown below, however, Plaintiffs' claims under those statutes fail, and Plaintiffs' "unlawful" theory dies with it. *Sybersound Records, Inc. v. UAV Corp.*, 517 F.3d 1137, 1152-53 (9th Cir. 2008) (dismissal of UCL claim proper because alleged conduct was not independently unlawful); *Avila v. Countrywide Home Loans*, 2010 WL 5071714, at *6 (N.D. Cal. Dec. 7, 2010) (dismissing UCL claim premised on violation of law for which plaintiff failed to state claim).

b. Plaintiffs Fail To Show "Unfair" Or "Fraudulent" Conduct.

Plaintiffs' claims of "unfair" and "fraudulent" conduct are one and the same, and fail for the same reasons. *Hadley v. Kellogg Sales Co.*, 2017 WL 1065293, at *20 (N.D. Cal. Mar. 21, 2017)

("[W]here the unfair business practices alleged under the unfair prong of the UCL overlap entirely with the business practices addressed in the fraudulent and unlawful prongs of the UCL, the unfair prong of the UCL cannot survive if the claims under the other two prongs of the UCL do not survive."). Plaintiffs claim Defendants are liable for stating on their websites that "'protecting our systems and our users' information is paramount to ensuring [Defendants'] users enjoy a secure user experience and maintaining our users' trust' and by representing that it had 'physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you.'" Compl. ¶¶ 128, 215. But those bare, generalized and "conclusory allegations do not support a claim" under the "unfair" prong that "Defendants' actions offend[] an established public policy or that they are immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers." *Buena Vista, LLC v. New Res. Bank*, 2010 WL 3448561, at *6 (N.D. Cal. Aug. 31, 2010) (quotations omitted); *see also Smith & Hawken, Ltd. v. Gardendance, Inc.*, 2004 WL 2496163, at *6 (N.D. Cal. Nov. 5, 2004). Plaintiffs cite no "established public policy" that Defendants violated by virtue of being the targeted victim of a state-sponsored hack. Moreover, while the criminals who broke into Defendants' systems certainly engaged in conduct that is "immoral, unethical, oppressive, unscrupulous or substantially injurious," the same is not true of Defendants, which themselves were the victims of a crime. *See*, *e.g.*, *Emery v. Visa Internat. Serv. Ass'n*, 95 Cal. App. 4th 952, 964 (2002) (plaintiff could not "impose liability on VISA because it failed to stop lottery merchants from improperly using its mark"); *In re Firearm Cases*, 126 Cal. App. 4th 959, 985 (2005) (defendants "did not control the wrongful acts [in question] or encourage others to engage in questionable acts").

Plaintiffs also fail to plead "fraudulent" conduct with particularity. *Kearns*, 567 F.3d at 1125. At most, the complained-of statements are aspirational goals, not specific and enforceable promises. Defendants' desire to place a "high priority" on user trust is non-actionable, and "[i]t is well-established that general statements about reputation, integrity, and compliance with ethical norms are inactionable 'puffery' …" *City of Pontiac Policemen's & Firemen's Ret. Sys. v. UBS AG*, 752 F.3d 173, 183 (2d Cir. 2014). Because Defendants made no specific or absolute promise of 100% security, the statements at issue must be seen as non-actionable puffery. *See Newcal Indus., Inc. v. Ikon Office Sol.*, 513 F.3d 1038, 1053 (9th Cir. 2008). Even if these statements could be

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

interpreted as more, Plaintiffs have failed to allege how the mere fact of a data breach proves them "fraudulent" (or "unfair"). Plaintiffs fail to specify: (1) the "safeguards" or "federal regulations" to which they refer; (2) how those "safeguards" failed to comply with "federal regulations;" or (3) how, if at all, Defendants knew the same when they made the alleged representations. *In re Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 991 (N.D. Cal. 2016). To the extent Plaintiffs attempt to craft actionable fraud from the alleged failure to disclose potential security vulnerabilities, Defendants' express statements that the network is not "100% secure" and has "inherent limitations" negate any such claim, or any obligation to further qualify or disclose potential vulnerabilities. *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1052 (N.D. Cal. 2014); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig. ("Sony I")*, 903 F. Supp. 2d 942, 969-70 (S.D. Cal. 2012) (dismissing UCL claim based on similar disclosures).

c. Plaintiffs Cannot Plead Reliance Necessary For Their UCL Claim.

Plaintiffs' failure to plausibly plead actual reliance is also fatal to their UCL claim sounding in fraud. *In re Tobacco II Cases*, 46 Cal. 4th 298, 326 (2009). Plaintiffs fail to meet that requirement on two fronts. *First*, although Plaintiffs reference generalized statements made in Defendants' Privacy Policies and on the "Security at Yahoo" webpage (*see*, *e.g.*, Compl. ¶ 128 n.74), they "never allege that they were aware of the privacy policy [or the "Security at Yahoo" webpage], let alone saw or read it." *Low II*, 900 F. Supp. 2d at 1027. As this Court has held, the "lack of allegations that a plaintiff had read an alleged false representation" justifies dismissal. *Id.* (citing *Durell v. Sharp Healthcare*, 183 Cal. App. 4th 1350, 1363 (2010) (the "[complaint] does not allege Durell ever visited Sharp's Web site or even that he ever read the Agreement for Services.")). "Without an allegation that Plaintiffs were somehow aware of contents of [Yahoo]'s privacy policy [or the "Security at Yahoo" webpage], … Plaintiffs cannot allege [Defendants'] misrepresentations were an immediate cause of the injury-causing conduct." *Id.* (quotations omitted).

Second, even if Plaintiffs had read these statements on Defendants' websites, they still would not be able to establish reliance (or falsity). Defendants' TOS disclaimed any notion that their "SERVICES OR SOFTWARE WILL BE UNINTERRUPTED, TIMELY, *SECURE* OR ERROR-FREE." Compl., Exh. 1, at 91 § 19(b); *id.*, Exh. 2, at 171 § 12 (d) (emphasis added). On top of that,

Yahoo disclosed that its services would not be "100% secure," and Aabaco warned that its "SECURITY MECHANISMS IN THE SERVICES HAVE INHERENT LIMITATIONS." RJN, Exh. A, at 1; Compl., Exh. 2, at 171 § 12(c).[21]

d. Plaintiffs Are Not Entitled To The Remedies Sought.

Plaintiffs additionally fail to plead any entitlement to the relief they seek. Restitution—not damages—is the only monetary relief available under the UCL. *Madrid v. Perot Sys. Corp.*, 130 Cal. App. 4th 440, 452 (2005); *Chamberlan v. Ford Motor Co.*, 2003 WL 25751413, at *9 (N.D. Cal. Aug. 6, 2003) (disallowing recovery because plaintiffs "ha[d] not alleged that they paid any money to Defendant"). Because the consumer Plaintiffs paid no money to use Yahoo's free email services, there is nothing to refund under a restitution theory. *Id.* Plaintiffs likewise cannot plead entitlement to injunctive relief, as they have failed to establish redressability. An "order requiring [Yahoo] to enhance [its] cybersecurity in the future (or an equivalent declaratory judgment) will not provide any relief for past injuries or injuries incurred in the future *because of a data breach that has already occurred*." *Dugas*, 2016 WL 6523428, at *8 (emphasis added).

2. Plaintiffs' Consumer Legal Remedies Act Claim Fails.

Plaintiffs claim Yahoo violated the CLRA when it "represented to Plaintiffs and the other Class members that its PII databases were secure and that customers' PII would remain private." Compl. ¶ 142. Plaintiffs are wrong on the facts and the law. *First*, Yahoo accounts are free, so Plaintiffs are not "consumers" under the CLRA.[22] They did not "purchase or lease" from Yahoo as required under the statute. *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 864 (N.D. Cal. 2011). *Second*, Yahoo provides a web-based, software driven, email platform, and as such does not provide a "good" or a "service" within the meaning of the CLRA. *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1070 (N.D. Cal. 2012). By definition, "goods" are statutorily limited to "tangible chattels," and "services" are specifically defined as "work, labor, and services … furnished in connection with sale or repair of [tangible chattels]." Cal. Civ. Code § 1761(a)-(b). Plainly, Yahoo

[21] Plaintiff Neff also cannot obtain injunctive relief because he admits he stopped using the service. Compl. ¶ 20; *Frenzel v. AliphCom*, 76 F. Supp. 3d 999, 1015 (N.D. Cal. 2014).

[22] Plaintiff Neff does not bring a CLRA claim. Nor could he, as he did not use any Yahoo services for "personal, family, or household purposes." Cal. Civ. Code § 1761(d). Rather, Neff used them "in connection with his online insurance agency business." Compl. ¶ 20.

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

accounts do not qualify, since email accounts are not "tangible chattel," and Yahoo does not provide any work or services in support of any tangible chattel. *Ferrington v. McAfee, Inc.,* 2010 WL 3910169, at *19 (N.D. Cal. Oct. 5, 2010) ("software [is] … not a service for purposes of the CLRA"). *Finally*, Plaintiffs do not claim to have read or relied on the allegedly misleading statements as a pre-condition of using Yahoo's free services. *Buckland v. Threshold Enters., Ltd.*, 155 Cal. App. 4th 798, 810 (2007) ("[P]laintiffs asserting CLRA claims … must establish they actually relied on the relevant representations or omissions."), *rev'd on other grounds by Kwikset*, 51 Cal. 4th 310. And if they had, they would have seen Yahoo's express disclosures that its services are not 100% secure.

3. Plaintiffs' Customer Records Act Claim Fails.

a. The Non-California Plaintiffs Lack Standing.

Non-California residents lack statutory standing to bring claims under the CRA (Cal. Civ. Code § 1798.80, *et seq.*). *See*, *e.g.*, *Sony I*, 903 F. Supp. 2d at 973 (dismissing CRA claim with prejudice and stating, "Plaintiffs try once again to save the claims of non-resident Plaintiffs, [but] the Breach Act is clear that it applies only to 'ensure the personal information [of] California residents [is] protected.'") (citing Cal. Civ. Code § 1798.81.5(a)); *see also Antman*, 2015 WL 6123054, at *5 (§ 1798.82 has procedures for notifying California residents); *Martinez v. Bank of Am., Corp.*, 2012 WL 3647434, at *9 (E.D. Cal. Aug. 23, 2012); *Garcia v. UnionBanCal Corp.*, 2006 WL 2619330, at *1 (N.D. Cal. Sept. 12, 2006); Cal. Civ. Code § 1798.82(a) (limiting notification to a "breach in the security of the data to a *resident of California*") (emphasis added). This statutory limitation cannot be enlarged by, or confused with, the application of California law to the claims of non-residents. *Fred Briggs Distrib. Co. v. Cal. Cooler, Inc.*, 1993 WL 306157 (9th Cir. Aug. 11, 1993) (rejecting argument that contractual California choice-of-law provision overrides jurisdictional limitations in statute restricting claims to California residents only). Here, only two Plaintiffs (Heines and Dugas (Compl. ¶¶ 10, 12)) allege they are California residents.[23] The remainder of the non-resident

[23] Statutory standing is "properly viewed as a dismissal for failure to state a claim rather than a dismissal for lack of subject[-]matter jurisdiction." *DB Healthcare, LLC v. Blue Cross Blue Shield of Ariz., Inc.*, 852 F.3d 868, 873 (9th Cir. 2017) (quotations omitted).

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Plaintiffs who assert CRA claims (Essar, the Ridolfos, Garg, Rivlin, Granot and Neff (Compl. ¶¶ 11, 13-16, 20)) lack statutory standing, and their claims must be dismissed.

b. CRA Notice Was Not Required For The 2013 Breach.

CRA notice was not required for California residents potentially affected by the 2013 Breach—a conclusion that can be reached by examining the CRA as it existed in 2013 and as amended in 2014.[24] In construing the CRA, the Court's "fundamental task … is to ascertain the intent of the lawmakers so as to effectuate the purpose of the statute." *Day v. City of Fontana*, 25 Cal. 4th 268, 272 (2001). Words must be given their usual and ordinary meaning unless the statutory terms are ambiguous. *Id.* "In such circumstances, [the court] select[s] the construction that comports most closely with the apparent intent of the Legislature, with a view to promoting rather than defeating the general purpose of the statute." *Id.* During the time of the 2013 Breach, the plain language of the CRA narrowly defined "personal information" under Section 1798.82(h), and it did not include "online account" information:

> [A]n individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
>
> (1) Social security number.
>
> (2) Driver's license number or California Identification Card number.
>
> (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
>
> (4) Medical information.
>
> (5) Health insurance information.

That narrow construction is supported by a later amendment to that same provision (effective January 1, 2014), which amended the definition of "personal information" to include online accounts, such as Defendants' services here.

Specifically, the Legislature amended the CRA's "definition of personal information, by adding certain information that would permit access to an *online account*." *See* RJN, Exh. M, at 1 (Legis. Counsel's Dig., Sen. Bill No. 46 (2012-2013 Reg. Sess.) (emphasis added) (acknowledging

[24] Neither Heines nor Dugas specifically claim they were affected by the 2013 Breach—Heines alleges to have received notice of the 2014 breach only (Compl. ¶ 10), and Dugas does not allege that he received notice regarding any of the Data Breaches (*id.* ¶ 12).

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

that usernames and passwords of online accounts fall outside of 2013 CRA); RJN, Exh. N, at 1-2 (Assem. Com. Jud., Analysis of Sen. Bill No. 46 (2012-2013 Reg. Sess.) as amended April 15, 2013); RJN, Exh. O, at 1 (Privacy Rights Clearinghouse Letter to Sen. Corbett dated April 16, 2013) ("Some of the most prominent breaches reported by the media in recent years have included data elements such as usernames and passwords, *not covered by California's data breach law*.") (emphasis added). The legislative record states that, "[d]espite the rise in online banking, shopping and other financial transactions, … private businesses are *not required* to give notification of a data breach when a user name, security question or password are compromised." RJN, Exh. P, at 1 (Assem. App. Com., Analysis of Sen. Bill No. 46 (2012-2013 Reg. Sess.) as amended April 15, 2013) (emphasis added); *see also* RJN, Exh. Q, at 1 (Assem. Jud. Com., Mand. Info. Worksheet, Sen. Bill No. 46 (2012-2013 Reg. Sess.) as amended April 15, 2013) ("Though notification requirements already exist whenever unencrypted Social Security numbers or driver's license numbers are stolen, for example, no similar protection exists when passwords and usernames, in combination with security questions/answers, are improperly changed or accessed.").

This Court may consider the amendment to the CRA—as well as the foregoing legislative materials and history concerning that amendment—to determine the Legislature's original intent in enacting the CRA. *See McClung v. Emp't Dev. Dept.*, 34 Cal. 4th 467, 473 (2004) ("[A] declaration of a later Legislature as to what an earlier Legislature intended is entitled to consideration."); *see also* Cal. Gov. Code § 9080(a) ("[L]egislative records relating to bills, resolutions, or proposed constitutional amendments before the Legislature provide evidence of legislative intent that may be important in the subsequent interpretation of laws enacted in the Legislature."). And when the Court considers those materials, along with the language of the statute as it existed in 2013, they compel one conclusion only—CRA notice was not required at the time of the 2013 Breach because Plaintiffs' claim concerns "online account information," which was not covered by the CRA at the time of the 2013 Breach.

In particular, the Complaint alleges that "hackers stole the names, email addresses, telephone numbers, birth dates, passwords, and security questions of Yahoo account holders." Compl. ¶ 1. This stolen information concerned customers' online accounts with Yahoo, *not* their "financial"

accounts. Indeed, Plaintiffs admit that "Yahoo asserts that the Breaches did not expose credit card data." *Id.* ¶ 58. Accordingly, the 2013 Breach involved the compromise of information regarding "online accounts," which was not in the operative version of the CRA during the 2013 Breach.

Plaintiffs cannot retroactively apply the amended version of the CRA to their claims. A "new statute is presumed to operate prospectively absent an express declaration of retrospectivity or a clear indication that the electorate, or the Legislature, intended otherwise." *See*, *e.g.*, *Doe v. Schwarzenegger*, 2007 WL 601977, at *1 (N.D. Cal. Feb. 22, 2007) (quoting *Tapia v. Superior Court*, 53 Cal. 3d 282, 287 (1991)). And there has been no express declaration of retrospectivity here. The CRA breach notice claim concerning the 2013 Breach therefore should be dismissed.

c. The CRA Does Not Apply To The "Forged Cookie Breach."

The CRA notice requirement does not apply to the Forged Cookie Breach because it does not involve exposure of the statutory data elements of "personal information" under Section 1798.82(h)(2).[25] Although Plaintiffs do not explain how the "forged cookie" process works, they do allege that the "attackers in this case … were able to forge these authentication cookies, which granted them access to targeted accounts without needing to supply the account's password." Compl. ¶ 68.[26] Section 1798.82(h)(2), however, requires breach notification of "online accounts" for specific data elements: a "user name or email address, in combination with a password or security question and answer that would permit access to an online account." Plaintiffs do not allege that the cookies contained any of those data elements, either alone or in combination. Although Plaintiffs do ask the Court to take several inferential leaps to assert potential Yahoo account access, they do *not* allege access using the statutorily-identified data elements.

[25] A "'cookie' is a small text file that a server creates and sends to a browser, which then stores the file in a particular directory on an individual's computer." *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 926 (N.D. Cal. 2015). "A cookie contains a limited amount of information which can relate to the browser or to a specific individual." *Id.* "When an individual using a web browser contacts a server—often represented by a particular webpage or internet address—the browser software checks to see if that server has previously set any cookies on the individual's computer." *Id.* "If the server recognizes any valid, unexpired cookies, then the computer 'sends' those cookies to the server." *Id.* "After examining the information stored in the cookie, the server knows if it is interacting with a computer with which it has interacted before." *Id.*

[26] Again, as a foundational matter, what Plaintiffs fail to allege also is key: no California-resident Plaintiff specifically claims to have been affected by the Forged Cookie Breach. Compl. ¶¶ 10, 12.

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

d. Plaintiffs Fail To Allege Damages Resulting From Any Allegedly Delayed Notice.

Even if a Plaintiff is a California resident and notice were required, the CRA claim nevertheless fails. Delay in notification is not enough to state a claim under the CRA. Instead, Plaintiffs must "allege that the damages *flowed from the delay*, and not just that the damage flowed from the intrusion." *In re Sony Gaming Networks & Customer Data Sec. Breach Litig. ("Sony II")*, 996 F. Supp. 2d 942, 1010 (S.D. Cal. 2014) (emphasis added) (dismissing breach-notification delay claim on similar grounds); *see also Dugas*, 2016 WL 6523428, at *7 (dismissing CRA claims under Rules 12(b)(1) and 12(b)(6) where "Plaintiff has failed to trace any harm from … delayed notification or to demonstrate a nexus between the alleged harm flowing from the delayed notification and Defendants' actions"); *Corona v. Sony Pictures Entm't, Inc.*, 2015 WL 3916744, at *9 (C.D. Cal. June 15, 2015) ("Plaintiffs have not alleged direct economic damages resulting from Sony's alleged failure to timely notify."); *Adobe*, 66 F. Supp. 3d at 1217-18 (dismissing Section 1798.82 claim when plaintiffs failed to allege any incremental harm purportedly suffered as a result of a notification delay); *In re Barnes & Noble Pin Pad Litig.*, 2016 WL 5720370, at *8 (N.D. Ill. Oct. 3, 2016) (dismissing CRA claim because plaintiff failed to "allege that her injuries were caused by the delay between the time she was notified of the breach and the time she contends she should have been notified.").

Here, Plaintiffs have not pled facts showing how they were injured specifically as a result of Defendants' purported notification delay. Rather, they at most allege damages that flow from the Data Breaches themselves, not from any lack of notice. Compl. ¶ 157 (addressing alleged harm from the compromise, not an alleged delay). Plaintiffs' failure to do so requires dismissal of the CRA claim. *Boorstein v. CBS Interactive, Inc.*, 222 Cal. App. 4th 456, 466-67 (2013).

e. Plaintiffs Have No Basis To Recover Statutory Penalties.

Even if Plaintiffs could allege sufficient notification-delay damages, they request statutory penalties under Section 1798.84(c) that are inapplicable here. Compl. ¶ 158. Section 1798.84(c) expressly limits the availability of statutory penalties to violations of Section 1798.83. Section 1798.83 is California's "Shine the Light" Law and concerns how a covered entity may "disclose customers' personal information to third parties for direct marketing purposes." *Miller v. Hearst*

Commc'ns Inc., 554 F. App'x 657, 658 (9th Cir. 2014); *King v. Conde Nast Publ'n*, 554 F. App'x 545, 546 (9th Cir. 2014). Plaintiffs, however, do not claim a violation of Section 1798.83 or that the Data Breaches concern disclosures to third parties for direct marketing purposes. Rather, Plaintiffs limit their allegations to claimed violations of Section 1798.82, which addresses data breach notification. Therefore, Plaintiffs' request for statutory penalties under Section 1798.84(b) should be dismissed. Finally, the same reasons that injunctive relief should be denied as stated in the UCL section apply equally here. The relief is unspecified and would impermissibly affect only past harm.

4. Plaintiffs' Stored Communications Act Claim Fails.

Plaintiffs concede (Compl. ¶¶ 162, 166) that the SCA requires that Yahoo and Aabaco "*knowingly* divulged" protected information. 18 U.S.C. § 2702 (emphasis added). But they admit "hackers stole" the information in question, not that Yahoo disclosed it to them or anyone else. *See*, *e.g.*, Compl. ¶ 1. At most, Plaintiffs claim Yahoo allegedly failed to take "commercially reasonable steps to safeguard" "sensitive" customer information. *Id.* ¶¶ 165, 170. But reasonableness is not the standard. As a matter of law, even "'reckless' or 'negligent' conduct is not sufficient." *Long v. Insight Commc'ns of Cent. Ohio, LLC*, 804 F.3d 791, 797 (6th Cir. 2015). Therefore, in cases where the defendant is the victim of the disclosure—rather than the perpetrator of it—courts routinely dismiss SCA claims for lack of willfulness. *See*, *e.g.*, *Willingham v. Glob. Payments, Inc.*, 2013 WL 440702, at *12 (N.D. Ga. Feb. 5, 2013) (dismissing SCA claim, in part, because hacked entity did not knowingly divulge information); *Worix v. MedAssets, Inc.*, 857 F. Supp. 2d 699, 703 (N.D. Ill. 2012) (dismissing SCA claim in data breach case and stating that the "SCA requires proof that the defendant 'knowingly divulge[d]' covered information, not merely that the defendant knowingly failed to protect the data … And the failure to take reasonable steps to safeguard data does not, without more, amount to divulging that data knowingly."); *Muskovich v. Crowell*, 1996 WL 707008, at *5 (S.D. Iowa Aug. 30, 1996) (employer whose failure to implement safeguards had resulted in data breach did not "knowingly divulge" because "[a]wareness of a 'possibility' does not rise to the level of a 'substantial certainty' required for liability under the [SCA]"). Because Plaintiffs admit Yahoo did not knowingly or voluntarily disclose information, their SCA claim fails.

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Moreover, the SCA distinguishes between "content" and "transactional" information, and a plaintiff must plausibly plead the intentional disclosure of the former to state a claim. However, Plaintiffs allege no facts showing that the information contained in the cookies or the "names, email addresses, telephone numbers, birth dates, passwords,[27] and security questions" (Compl. ¶ 1) alleged to have been stolen qualify as "contents," as opposed to other transactional or otherwise automatically generated data. No Plaintiff specifically claims to have been affected by the Forged Cookie Breach. Regardless, the information at issue in the Forged Cookie Breach such as "user identification information, records of session times and durations and temporarily assigned network addresses … is not considered to be content-based." *Obodai v. Indeed, Inc.*, 2013 WL 1191267, at *3 (N.D. Cal. Mar. 21, 2013) (quotations omitted); *see also In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014) ("'contents' … does not include record information regarding the characteristics of the message that is generated in the course of the communication."); *iPhone*, 844 F. Supp. 2d at 1061 (dismissing SCA claim and finding data at issue "is generated automatically, rather than through the intent of the user, and therefore does not constitute 'content'"). None of the information Plaintiffs allege was stolen from Yahoo as part of the Data Breaches qualifies as "content" within the meaning of the SCA. Nor is it sufficient if the stolen information allowed a hacker to piece together data and then access a customer's personally identifiable information. *Zynga*, 750 F.3d at 1107 ("There is no language in [the SCA] equating 'contents' with personally identifiable information. Thus, an allegation that Facebook and Zynga disclosed personally identifiable information is not equivalent to an allegation that they disclosed the contents of a communication."). Because the allegations do not include facts that the stolen information contained "contents" of a communication, Plaintiffs' SCA claim fails for this reason as well. *Sams v. Yahoo!, Inc.*, 2011 WL 1884633, at *7 (N.D. Cal. May 18, 2011) (dismissing SCA claim when plaintiff alleged only the disclosure of "non-content-based information").

5. Plaintiffs' Online Privacy Protection Act Claim Fails.

Plaintiffs' Online Privacy Protection Act ("OPPA") claim is fatally deficient. *First*, "the OPPA itself does not provide for a private action or public prosecution for any violation of its

[27] Yahoo's announcement specified that unprotected passwords were not stolen. *Supra* note 15.

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

provisions." *People ex rel. Harris v. Delta Air Lines, Inc.*, 247 Cal. App. 4th 884, 891 (2016) (addressing case brought by the State of California). Accordingly, Plaintiffs cannot assert a standalone OPPA claim. *Second*, to the extent Plaintiffs want to bootstrap a UCL claim to an alleged OPPA violation, Plaintiffs cannot extend that claim beyond California residents. OPPA governs "an operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers *residing in California* who use or visit its commercial Web site." Cal. Bus. & Prof. Code § 22575 (emphasis added); *see also* Cal. Bus. & Prof. Code § 22577 (defining regulated "operator" as one that "collects and maintains personally identifiable information from a consumer *residing in California*") (emphasis added). Here, only two Plaintiffs (Heines and Dugas (Compl. ¶¶ 10, 12)) are California residents. The remaining Plaintiffs are non-California residents and therefore lack statutory standing. *Finally*, even for the two California residents seeking to assert an OPPA violation as a predicate to a UCL claim, the attempt fails. Like the CLRA, OPPA is limited to "consumers" only, and neither Heines nor Dugas claim they "purchase[d] or lease[d], any goods, services, money, or credit for personal, family, or household purposes" from Yahoo. Compl. ¶¶ 10, 12; Cal. Bus. & Prof. Code § 22577(d). This is unsurprising because "Yahoo operates Yahoo Mail as a free web-based email service." *In re Yahoo Mail Litig.*, 2016 WL 4474612, at *1 (N.D. Cal. Aug. 25, 2016). Any California resident who used Yahoo's free services cannot be an OPPA "consumer."[28] Accordingly, no Plaintiff has a viable OPPA claim, either independently or as a predicate to a UCL claim.

6. Plaintiffs' Express Contract Claim Fails.

To state a claim for breach of contract, Plaintiffs must plead facts showing "the contract, plaintiffs' performance (or excuse for nonperformance), defendant's breach, and damage to plaintiff therefrom." *Low II*, 900 F. Supp. 2d at 1028 (quotations omitted). Plaintiffs reason from the fact of the intrusion itself to the faulty conclusion that Defendants somehow breached their "promises" that they would not willingly share Plaintiffs' personal information, and that they would attempt to

[28] Similarly, even if Neff (a Texas citizen who purports to sue on behalf of a "small business user class") were a California resident *and* paid for Yahoo services, his claims would fail for another independent reason: any plaintiff who solely alleges use of Yahoo's business products is not a "consumer" under this definition because business purposes are not "personal, family, or household purposes." Cal. Bus. & Prof. Code § 22577(d).

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

safeguard that information. Plaintiffs cannot, however, cherry-pick sentences and phrases from Defendants' public statements to stitch together a contract claim:

- "We are committed to ensuring your information is protected and apply safeguards in accordance with applicable law."
- "Yahoo does not rent, sell, or share personal information about you with other people or non-affiliated companies except to provide products or services you've requested, when we have your permission, or under [certain inapplicable circumstances]."
- "We limit access to personal information about you to employees who we reasonably believe need to come into contact with that information to provide products or services to you or in order to do their jobs."
- "We have physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you."

Compl. ¶ 179(a)-(d); *see also id.* ¶ 181(a)-(c) (alleging that Aabaco's Privacy Policy contained similar "promises"). Plaintiffs contend Yahoo and Aabaco broke those unilateral "promises" because they "did not have proper safeguards 'in accordance with applicable law' to protect Plaintiffs and Class members' 'Personal Information,' and did not limit access to that information to the specified individuals or entities." *Id.* ¶ 182. Plaintiffs likewise claim Yahoo and Aabaco "violated their commitment to maintain the confidentiality and security of the PII of Plaintiffs and the class members, and failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security." *Id.* Plaintiffs' allegations fall far short.

First, Plaintiffs grossly mischaracterize Defendants' statements. Yahoo and Aabaco never guaranteed Plaintiffs a completely secure, hack-proof environment. To the contrary, Yahoo explained that any use of the services would be "AT YOUR OWN RISK" and on an "AS IS" and "AS AVAILABLE" basis, it expressly disclaimed any warranties to the contrary, including that its services would be "SECURE," and it warned Plaintiffs that "no data transmission over the Internet or information storage technology can be guaranteed to be 100% secure." Compl., Exh. 1, at 91 § 19(a) & (b); RJN, Exh. 2. Aabaco similarly warned users that use of its services would be "AT YOUR OWN RISK," "AS IS" and "AS AVAILABLE," it disclaimed any warranties that its services would be "SECURE," and it expressly warned users that any "SECURITY MECHANISMS IN THE SERVICES HAVE INHERENT LIMITATIONS." Compl., Exh. 2, at 171 § 12(a), (c) & (d). Those

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

statements are the polar opposite of the promises Plaintiffs claim were made. This alone defeats Plaintiffs' contract claim. *Young v. Facebook, Inc.*, 790 F. Supp. 2d 1110, 1117 (N.D. Cal. 2011).

When Defendants' Privacy Policies, TOS and corresponding disclosures are read in the proper light, Plaintiffs cannot show a breach. They also plead no facts showing how Defendants: (1) failed to "apply safeguards in accordance with applicable law" (Compl. ¶ 179(a)); (2) "rent[ed], s[old], or share[d] personal information" about Plaintiffs (*id.* ¶¶ 179(b), 181(a)); (3) granted "access to personal information about [Plaintiffs]" to individuals who are not Yahoo employees (*id.* ¶¶ 179(c), 181(b)); or (4) implemented "physical, electronic, and procedural safeguards" that did not "comply with federal regulations" (*id.* ¶¶ 179(d), 181(c)). Neither Yahoo nor Aabaco affirmatively rented, sold, or shared Plaintiffs' personal information. Moreover, even "[i]f the breach of the parties' contract is [Yahoo and Aabaco]'s alleged failure to comply with federal law," Plaintiffs nonetheless fail to "plead the federal law or laws with which [Yahoo and Aabaco] allegedly did not comply" or how. *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1177 (D. Minn. 2014); *Anthem*, 162 F. Supp. 3d at 982.

Second, on top of the reasons stated in Section IV(A), Plaintiffs cannot establish the damages element of their claim. *Aguilera v. Pirelli Armstrong Tire Corp.*, 223 F.3d 1010, 1015 (9th Cir. 2000) (contract claims require "appreciable and actual damage."). The limitation of liability provisions in Defendants' TOS bar the precise damages Plaintiffs seek—damages they claim to be consequential to the Data Breaches. Compl. ¶ 184. Here, Yahoo's TOS contains a limitation of liability clause, which provides:

"YOU EXPRESSLY UNDERSTAND AND AGREE THAT YAHOO … SHALL NOT BE LIABLE TO YOU FOR ANY PUNITIVE, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES, INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, DATA OR OTHER INTANGIBLE LOSSES (EVEN IF YAHOO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES), RESULTING FROM: … UNAUTHORIZED ACCESS TO OR ALTERATION OF YOUR TRANSMISSIONS OR DATA … OR … ANY OTHER MATTER RELATING TO THE YAHOO SERVICE." Compl., Exh. 1, at 91.

Similarly, Aabaco's TOS contains an even broader limitation of liability clause:

"TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW, YOU EXPRESSLY UNDERSTAND AND AGREE THAT THE COMPANY … SHALL NOT BE LIABLE, UNDER ANY CIRCUMSTANCES OR LEGAL THEORIES WHATSOEVER, FOR

ANY INDIRECT, PUNITIVE, INCIDENTAL, SPECIAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES …" Compl., Exh. 2, at 172.

Because Plaintiffs plead no facts showing those provisions are unenforceable—only legal conclusions—they foreclose the damages element of Plaintiffs' contract claim. *See* Compl. ¶ 234. Indeed, these very types of limitations provisions are routinely enforced under California law, particularly where, as here, the service offered is free or at a low cost to the subscriber. *Food Safety Net Servs. v. Eco Safe Sys. USA, Inc.,* 209 Cal. App. 4th 1118, 1126 (2012); *Lewis v. YouTube, LLC*, 244 Cal. App. 4th 118, 125 (2015) (enforcing limitation of liability provisions for free service) (citing *Markborough Cal., Inc. v. Superior Court*, 227 Cal. App. 3d 705, 714 (1991)). For these reasons, Plaintiffs' express contract claim fails.

7. Plaintiffs' Implied Contract Claim Fails.

Plaintiffs admit their implied contract claim is wholly duplicative of their express contract claim. Compl. ¶ 186. That duplication requires dismissal. *O'Connor v. Uber Techs., Inc.*, 2013 WL 6354534, at *10 (N.D. Cal. Dec. 5, 2013). In addition, to plausibly allege that an implied contract existed beyond the express terms to which the parties agreed, Plaintiffs had to "elaborate upon the nature and scope of the implied contract in the pleadings," rather than simply declare one existed. *Anthem*, 162 F. Supp. 3d at 982-83; *Frezza v. Google Inc.*, 2012 WL 5877587, at *4 (N.D. Cal. Nov. 20, 2012).[29] They did not. Finally, as with their express contract claim, Plaintiffs cannot overcome the limitation of liability provisions in Defendants' TOS, or their failure to plead actual, concrete damage specifically caused by the alleged breach of any purported implied contract. *Lewis*, 244 Cal. App. 4th at 125-26. Accordingly, the implied contract claim fails.

8. Plaintiffs' Implied Covenant Claim Fails.

Plaintiffs' implied covenant claim suffers multiple infirmities, and it should be dismissed. As an initial matter, the claim stands and falls alongside Plaintiffs' express contract claim. *Northstar Fin. Advisors Inc. v. Schwab Invs.*, 135 F. Supp. 3d 1059, 1089 (N.D. Cal. 2015). Because Plaintiffs' express contract claim fails, so too does their implied covenant claim.

[29] To the extent Plaintiffs claim Defendants implicitly warranted against unauthorized access to their accounts, that claim is flatly refuted by Defendants' explicit disclaimer of any such warranties. Compl., Exh. 1, at 91; *id.*, Exh. 2, at 171.

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Nor can Plaintiffs add terms to any express agreements under an implied covenant theory. *Avidity Partners, LLC v. State*, 221 Cal. App. 4th 1180, 1204 (2013) (as a matter of law, the "implied covenant of good faith and fair dealing does not impose substantive terms and conditions beyond those to which the parties actually agreed"). Plaintiffs, however, seek to do precisely that here. They claim Defendants breached the implied covenant of good faith and fair dealing by: "(a) using password encryption standards that were long known to be unsafe; (b) taking no serious action in response to past breaches; (c) falling well behind industry standards of cybersecurity; and (d) under-investing in cybersecurity resources despite assurances to its users to the contrary." Compl. ¶ 193. Plaintiffs, however, cite no provisions in any agreement wherein Defendants promised to: (1) employ specific password encryption standards; (2) employ specific protocols in cases of suspected or confirmed breaches; (3) employ a particular set of cybersecurity standards; or (4) invest a particular sum of time or money in any "cybersecurity resources." Plaintiffs cannot rewrite the contract to impose these extra-contractual duties by way of an implied covenant claim. And to the extent Plaintiffs attempt simply to buttress their contract claims by alleging violation of the implied covenant, it must fail on that basis as well. *Careau & Co. v. Sec. Pac. Bus. Credit, Inc.,* 222 Cal. App. 3d 1371, 1395 (1990) (dismissing implied covenant claim that relies on same facts and alleged damages as contract claim).

Further, Plaintiffs cannot show "bad faith." To do so, Plaintiffs must show Defendants committed a "conscious and deliberate act, which unfairly frustrate[d] the purposes of the parties' written contract." *Hougue v. City of Holtville*, 2008 WL 1925249, at *4 (S.D. Cal. Apr. 30, 2008) (quotations omitted). Plaintiffs cannot make that showing for two reasons. *First*, Plaintiffs do not "identify the specific contractual provision that was frustrated." *Perez v. Wells Fargo Bank, N.A.*, 2011 WL 3809808, at *18 (N.D. Cal. Aug. 29, 2011). Plaintiffs claim they "were to benefit through the use of Defendants Yahoo and Aabaco's services." Compl. ¶ 192. But Plaintiffs *did* use those services, and nowhere do they allege that the Data Beaches deprived them of services due to Defendants' bad faith. *Second*, Plaintiffs fail to show how Defendants consciously and deliberately prevented such use. Instead, they claim Defendants engaged in bad faith by failing to assume a host

of extra-contractual duties. *Id.* ¶ 193. But, as stated above, those allegations cannot form the basis for a "bad faith" claim.

Finally, as with Plaintiffs' other contract theories, they cannot overcome the limitation of liability provisions in Defendants' TOS. *See*, *e.g.*, *Darnaa, LLC v. Google Inc.*, 2017 WL 679404, at *8 (N.D. Cal. Feb. 21, 2017) (limitation of liability provision barred implied covenant claim). The claim should be dismissed.

9. Plaintiff Brian Neff's Fraudulent Inducement Claim Fails.

Neff[30] fails to state a fraudulent inducement claim, much less with the requisite particularity. To do so, Neff had to show: (1) a misrepresentation; (2) knowledge of the falsity; (3) intent to defraud, *i.e.*, to induce reliance; (4) justifiable reliance; and (5) resulting damage. *Herskowitz v. Apple Inc.*, 940 F. Supp. 2d 1131, 1147 (N.D. Cal. 2013). He did not.

First, Neff broadly claims Defendants "made numerous representations, in advertising and in the Privacy Policy, regarding the supposed secure nature of their small business services." Compl. ¶ 198. Neff, however, fails to allege that he actually reviewed any portions of that "advertising," the "Terms of Service," or the "Privacy Policies." That alone is fatal.

Second, Neff does not plead falsity. He claims Defendants' non-specified "representations" were "false because Yahoo and Aabaco utilized outdated encryption protocols, and failed to disclose that they did not use reasonable, industry-standard means, to safeguard against hacking and theft of customer PII." Compl. ¶ 198. But Neff does not: (1) identify the particular "encryption protocols" or "industry standards" to which he refers; or (2) establish when, where and how Defendants promised to employ particular encryption protocols or conform to particular industry standards. Neff also fails to establish the falsity of any such representations when made. He claims he signed up for his Aabaco service in September of 2009. *Id.* ¶ 20. But he does not allege which "encryption protocols" Defendants used in September of 2009, how those "protocols" failed to meet a particular "industry standard" in September of 2009, or the factual basis for his claim that Defendants knew the same in September of 2009.

[30] Only Neff brought claims on behalf of the Small Business Users Class. Compl. ¶ 20.

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

Third, as stated above, Defendants openly disclosed that use of the services would be "AT YOUR OWN RISK" and on an "AS IS" and "AS AVAILABLE" basis, they expressly disclaimed any warranties to the contrary, including that the "SERVICES WILL … BE … SECURE," and they disclosed that the "SECURITY MECHANISMS IN THE SERVICES HAVE INHERENT LIMITATIONS." Compl., Exh. 2, at 171 § 12(a), (c) & (d). In light of those disclaimers, Neff cannot show falsity or reliance. *See*, *e.g.*, *Minkler v. Apple, Inc.*, 65 F. Supp. 3d 810, 821 (N.D. Cal. 2014) ("Plaintiff has failed to identify any specific statement by Apple that expressly indicates that Apple Maps would always work flawlessly and without error."); *Dix v. Nova Benefit Plans, LLC*, 2015 WL 12859221, at *7 (C.D. Cal. Apr. 28, 2015) ("A plaintiff cannot claim justifiable reliance where, as here, 'disclaimers … are more than sufficient to put a reasonably prudent [plaintiff] on notice that the [information] contained [in a document] should be verified by the [plaintiff's] independent' investigation.") (citations omitted).

10. Foreign Plaintiffs Cannot Assert A California Negligence Claim, And Negligence Is Barred By The Economic Loss Doctrine.

The Court also should dismiss the negligence claim brought by the Australia, Venezuela and Spain class representatives (the "Foreign Plaintiffs") under California law,[31] which mandates that the laws of New South Wales, Florida and Ireland, respectively, govern those claims exclusively.[32]

Under California law, choice-of-law provisions are presumptively valid and broadly construed to encompass tort claims. *Cannon v. Wells Fargo Bank, N.A.,* 917 F. Supp. 2d 1025, 1051-52 (N.D. Cal. 2013); *Smith, Valentino & Smith, Inc. v. Superior Court*, 17 Cal. 3d 491, 494 (1976) ("[C]hoice of law provisions are usually respected by California courts."). Here, the Foreign Plaintiffs contracted with "various foreign Yahoo subsidiaries, many of which had differing Terms of Service." Compl. ¶ 122. The Australia UTOS states that "the TOS and the relationship between

[31] Because the Foreign Plaintiffs originally filed their individual claims in California, California choice-of-law rules apply. *Sony II*, 996 F. Supp. 2d at 977 (federal court sitting in diversity "must apply the choice-of-law rules of each state where the individual actions were originally filed.").

[32] In addition to the ATOS, the Foreign Plaintiffs were bound by Yahoo's UTOS, which is incorporated by reference into the ATOS. The Israel Class is excluded from the definition of "Foreign Plaintiffs" because the UTOS and ATOS stipulates that California law applies to persons using Israeli services, and that exclusive jurisdiction and venue is limited to Santa Clara County, or the Northern District of California. *Infra* note 34, at 10.

you and Yahoo shall be governed by the laws of New South Wales without regard to its conflict of law provisions."[33] The Australia ATOS includes even stricter language, requiring that "the laws of New South Wales govern not only the interpretation of this ATOS … but also apply to *all other claims, including claims regarding consumer protection laws, unfair competition laws, and in tort.*" (Emphasis added).[34] The Venezuela ATOS and UTOS contain language identical to the Australia agreements, except they require application of Florida law.[35] Finally, the Spain ATOS, which the UTOS incorporates by reference, states that "the laws of Ireland govern this ATOS and *any non-contractual obligations* arising out of it."[36] (Emphasis added). Thus, the Foreign Plaintiffs' negligence claim exists only "because of" the UTOS and ATOS into which they entered. *Nedlloyd Lines B.V. v. Superior Courts*, 3 Cal. 4th 459, 469-70 (1992). Accordingly, the UTOS and ATOS agreements should be enforced, and the negligence claim dismissed.

But even if the Foreign Plaintiffs could assert a claim for negligence under California law, the claim would still fail. Under California law, Plaintiffs' claims for negligent misrepresentation (including the negligent misrepresentation claim brought by Neff)[37] and negligence are barred by the economic loss rule because the claimed damages are not "accompanied by some form of physical harm (*i.e.*, personal injury or property damage)." *Sony I*, 903 F. Supp. 2d at 961; *see also Strumlauf v. Starbucks Corp.*, 192 F. Supp. 3d 1025, 1036 (N.D. Cal. 2016); *Minkler*, 65 F. Supp. 3d at 820; *Dugas*, 2016 WL 6523428, at *12.[38] Plaintiffs' failure to allege such harm warrants dismissal.

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

[33] RJN, Exh. B, at 1, https://policies.yahoo.com/au/en/yahoo/terms/utos/index.htm.

[34] RJN, Exh. C, at 9, https://policies.yahoo.com/xw/en/yahoo/terms/product-atos/comms/index.htm.

[35] *Id.* at 5; RJN, Exh. D, at 7, https://policies.yahoo.com/e2/es/yahoo/terms/utos/index.htm.

[36] *Supra* note 34, at 5.

[37] Neff's negligent misrepresentation claim mirrors his fraudulent inducement claim, and, as a consequence, it suffers the same infirmities. It should be dismissed for the same reasons.

[38] Indeed, the Foreign Plaintiffs likely crafted their claim as one sounding in negligence, as opposed to contract, in a misguided attempt to avoid the various TOS to which they agreed, which require them to bring their claims under different laws and in different fora. The economic loss rule, however, prevents that very tactic—*i.e.*, recasting contract claims as tort claims.

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

11. Foreign Plaintiffs' Claims Should Be Dismissed For *Forum Non Conveniens*.

The Foreign Plaintiffs should be dismissed from this lawsuit for the additional, independent reason that they agreed to litigate their claims elsewhere. The same TOS that requires the Foreign Plaintiffs to bring their negligence claim under the laws of different jurisdictions also compels each to bring his or her claims in those jurisdictions. *See supra*, notes 33-36. As a consequence, under the doctrine of *forum non conveniens*, the Foreign Plaintiffs should be dismissed from this lawsuit.

Under a traditional *forum non conveniens* analysis where there is no forum selection clause, courts must evaluate the convenience of the parties (*i.e.*, private interest factors) and various public interest factors. *Atl. Marine Constr. Co., Inc. v. U.S. Dist. Ct. for W. Dist. of Tex.*, 134 S. Ct. 568, 581 (2013). But where, as here, the parties' contract contains a valid forum selection clause, that "clause [should be] given controlling weight in all but the most exceptional cases." *Id.* (quotations omitted). Thus, a forum selection clause changes the *forum non conveniens* analysis in three ways: (1) the plaintiff's forum choice merits no weight; (2) the court does not consider the parties' private interests and deems those factors to weigh entirely in favor of the preselected forum; and (3) the agreed-upon forum need not apply the law of the court where the suit was filed. *Id.* at 581-82. "As a consequence, a district court may consider arguments about public-interest factors only." *Id.* at 582. "Because those factors will rarely defeat a transfer motion, the practical result is that forum-selection clauses should control except in unusual cases." *Id.* In sum, the Foreign Plaintiffs have a "heavy burden to show that this is the exceptional or unusual case." *Acceler-Ray, Inc. v. IPG Photonics Corp.*, 2017 WL 1196835, at *5 (N.D. Cal. Mar. 31, 2017). They cannot meet that burden.

The Foreign Plaintiffs cannot remotely show the public interest factors merit disregarding the contractual terms—*i.e.*, the administrative difficulties flowing from court congestion, the local interest in having localized controversies decided at home, and the interest in having the trial in a forum that is at home with the law. *Atl. Marine*, 134 S. Ct. at 581 n.6. California has little to no interest in hearing disputes brought by citizens of Australia, Spain and Venezuela, particularly when those individuals agreed to litigate in fora in or closer to their respective residences. Courts in Australia, Ireland and Florida unquestionably are more familiar with the laws of their respective jurisdictions, and no one disputes that the Northern District of California has one of the most heavily

congested dockets in the country. In the end, this is not an "unusual case" where "public-interest factors overwhelmingly disfavor a transfer." *Id.* at 583. The Foreign Plaintiffs should be dismissed from this lawsuit so they can bring their negligence claims where they belong—in the jurisdictions to which they agreed.

12. Plaintiffs' Declaratory Relief Claim Fails.

The declaratory relief claim should be dismissed. To start, Plaintiffs claim five provisions of Defendants' respective TOS are "unconscionable and unenforceable." Compl. ¶ 234. Although the burden is on Plaintiffs to establish both procedural and substantive unconscionability, Plaintiffs here plead no *facts* to support either prong. *Poublon v. C.H. Robinson Co.*, 846 F.3d 1251, 1260 (9th Cir. 2017) (party opposing contractual enforcement bears the burden to establish procedural and substantive unconscionability). Nor can they. At most, Plaintiffs have offered nothing save "threadbare recitals" and "bald assertions." This does not pass pleading muster. *Biggins v. Wells Fargo & Co.*, 266 F.R.D. 399, 412 (N.D. Cal. 2009) (allegation that contractual terms are "onerous to the point of being unconscionable" is "a bare legal conclusion unsupported by facts").

Nor could Plaintiffs plead sufficient facts. Indeed, their very request ignores the fact that Defendants expressly disclaimed *any* warranty about the security of their services, and this Court recently enforced a similar disclaimer in *Davidson v. Apple, Inc.*, 2017 WL 976048 (N.D. Cal. Mar. 14, 2017). As in *Davidson*, Defendants "disclaimed all implied warranties in accordance with California law because [they] stated in clear language and capitalized formatting" that they were expressly disclaiming "all warranties of any kind, whether express or implied, including, but not limited to the implied warranties of title, merchantability, fitness for a particular purpose and non-infringement." *Id.* at *15; *see also* Compl., Exh. 1, at 91; *accord Sony II*, 996 F. Supp. 2d at 983 (dismissing warranty claims "based on the disclaimer in the PSN User Agreement and the PSN Privacy Policy"). As in *Davidson*, Plaintiffs make "no allegations that Plaintiffs did not see or understand the [TOS]'s implied warranty disclaimer, or that Plaintiffs were surprised by the disclaimer's terms." *Davidson*, 2017 WL 976048 at *15. Plus, as stated above, "[l]imitation of liability clauses have long been recognized as valid in California." *Lewis*, 244 Cal. App. 4th at 125

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627

(quotations omitted); *Markborough*, 227 Cal. App. 3d at 714; *Darnaa, LLC v. Google, Inc.*, 2015 WL 7753406, at *3 (N.D. Cal. Dec. 2, 2015).

Further, the vague allegation that the disputed provisions are "precluded" by unspecified "federal and state law" (Compl. ¶ 234) is insufficient. *See Anthem*, 162 F. Supp. 3d at 982 (claim failed based on unspecific allegations that defendants "were required to comply with 'federal and state laws and regulations, including HIPAA, and industry standards'"); *Target*, 66 F. Supp. 3d at 1177 (finding if data breach claim is based on "Target's alleged failure to comply with federal law, … Plaintiffs must plead the federal law or laws with which Target allegedly did not comply").

Finally, this claim merely anticipates an affirmative defense under Yahoo and Aabaco's respective TOS, duplicates Plaintiffs' contractual clauses of actions, and is therefore improper. *J&J Sports Prods., Inc. v. Sally & Henry's Doghouse Bar & Grill LLC*, 2016 WL 1323464, at *2 (S.D. Cal. Apr. 4, 2016); *PhotoThera, Inc. v. Oron*, 2007 WL 4259181, at *3 (S.D. Cal. Dec. 4, 2007); *In re Zappos.com, Inc.*, 2013 WL 4830497, at *5 (D. Nev. Sept. 9, 2013) ("The Court dismisses this [data breach declaratory relief] claim, as it is on its face duplicative of the causes of action elsewhere directly asserted.").

V. CONCLUSION

For these reasons, the Court can and should dismiss Plaintiffs' entire Complaint. Because the stated defects are irremediable, the dismissal should be with prejudice.

Dated: May 22, 2017

HUNTON & WILLIAMS LLP

By: /s/ Ann Marie Mortimer
Ann Marie Mortimer
Attorneys for Defendants
Yahoo! Inc. and Aabaco Small Business, LLC

Hunton & Williams LLP
550 South Hope Street, Suite 2000
Los Angeles, California 90071-2627